REMARKS

Claims 1-32 are pending in the present application. No claims have been amended. Applicant believes that the present application is in condition for allowance, and respectfully requests reconsideration of the rejection in light of the remarks set forth below.

I. REJECTION UNDER 35 U.S.C. §102

The Office Action rejected claims 17 and 30-32 under 35 U.S.C. §102(b) as being allegedly anticipated by U.S. Patent No. 6,707,915 issued to Jobst. The rejection is respectfully traversed in its entirety.

To anticipate a claim under 35 U.S.C. § 102(b), the reference must teach every element of the claim and "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." (see MPEP §2131).

The Office Action states that Jobst teaches every element of claims 17 and 30-32. Applicant respectfully disagrees with the characterization of Jobst for the following reasons.

Claims 17 and 30-32 may be understood based on FIG. 3, in which the claimed "apparatus" or "device" may be the Token 230 which is coupled to the mobile station 220. The Token 230 has a key UAK 320 that is held private from the mobile station 220. The Token 230 also receives a secondary signature 340 from the mobile station 220. The Token 230 then generates (in signature generator 360) a primary signature 370 based on both the key UAK 320 and secondary signature 340. The primary signature 370 is then sent to the mobile station 220 (and subsequently to the network 210) for authenticating the subscriber.

Jobst discusses a method for securely transferring a data packet from a software provider to a requesting terminal. Public key encryption (i.e., public-private key pairs) is used to secure and verify the software downloaded by the requesting terminal from the software provider. (Col. 11, lines 24-31) The software provider generates a signature (sig1) over each data block of software being transmitted. (Col. 11, lines 36-39) The signature (sig1) is then encrypted using its private key 64 (Col. 11, lines 39-41) and appended to the data block being sent to the requesting terminal (Col. 11, lines 42-43). At the requesting terminal the data block and appended encrypted signature are received. The requesting terminal decrypts the received encrypted signature (using the public key for the software provider). The requesting terminal also recalculates a local version of the signature (sig1') over the data block. (Col. 11, lines 51-54). The local version of the signature (sig1') is compared to the receiver signature (sig1) verify the data block. (Col. 11, lines 56-59). Consequently, Jobst merely discloses a method that uses conventional public-private key protection.

The Office Action asserts that Jobst (Col. 11, lines 32-43) discloses generating a primary signature (i.e., sig1) based upon a key (i.e., private key 64) and a secondary signature (i.e., sig1') that is received from the mobile station. A close reading of Jobst discloses that the primary signature (i.e., sig1) is not generated based on the private key 64 but is merely encrypted using the private key 64. (See Col. 11, lines 39-41 - "This signature [sig1] 62 is then encrypted using the private key 64 ...") Therefore, Jobst does not disclose the limitation of "generating a primary signature based on a key that is held private ..." as claimed. Consequently, Jobst fails to disclose this limitation.

Additionally, the Office Action asserts that Jobst (Col. 11, lines 32-43 and lines 50-59) discloses "receiving a secondary signature (i.e., sig1;) from a mobile station" and that the

"primary signature is based on (both) the key ... and the secondary signature (sig1'). However, as noted above, the primary signature (sig1) of Jobst is computed at the software provider 33. The mobile terminal never sends the secondary signature (sig1') to the software provider 33. Therefore, the primary signature (sig1) of Jobst cannot be based on the secondary signature (sig1'). Instead, the mobile station (requesting terminal) of Jobst computes the signature sig1' as a local version of the received signature sig1 to verify that integrity of the data block received from the software provider. (See Col. 11, lines 51-59) The mobile station (requesting terminal) never sends the secondary signature (sig1') to the software provider. Consequently, Jobst fails to disclose this limitation.

Moreover, the present claims recite that "the primary signature is conveyed to the mobile station for authenticating the subscriber." However, the primary signature (sig1) of Jobst does not authenticate the *subscriber*. Instead, the signature (sig1) merely serves to verify the integrity or authenticity of the data block received from the software provider. (See Col. 11, lines 51-59) In Jobst, if the signatures (sig1 and sig1') match the received data block is considered to be error free. If the signatures do not match, the received data block is considered to have errors. Consequently, comparing the two signatures sig1 and sig1' in Jobst is different than generating and using the primary signature for authentication as claimed. Consequently, Jobst fails to disclose this limitation.

Lastly, Applicant notes that the cited prior art often refers to machine-to-machine authentication. In other words, the authentication takes place as to the machine itself and *not the user of that machine*. By contrast, the present claimed invention is aimed at an apparatus for *authenticating* a *subscriber or user* in a wireless communication system. With authentication the verifier or apparatus is able to determine whether the mobile user device is who he says he is.

By contrast, in security implementation, such as data encryption, a recipient of encrypted data either decrypts or fails to decrypt data but does not provide the sender of the data any information about whether such recipient is valid or authorized. Consequently, the claimed authentication method is distinct from prior art data security mechanisms.

Consequently, Jobst fails to disclose the generation of a secondary signature as in the claimed authentication method.

Since Jobst does not disclose at least the above elements of claims 17 and 30-32, Applicant submits that Jobst does not teach all elements of claims 17 and 30-32 and therefore, claims 17 and 30-32 are allowable.

For at least the foregoing reasons, Applicant respectfully submits that Jobst does not teach every element of the claims and requests a withdrawal of the rejection under 35 U.S.C. §102.

Applicant has reviewed the references made of record and asserts that the pending claims are patentable over the references made of record.

II. ALLOWED CLAIMS

Applicant notes with appreciation the Examiner's allowance of claims 1-16 and 18-29 and request that they be promptly issued.

CONCLUSION

In light of the remarks contained herein, Applicant submits that the application is in condition for allowance, for which early action is requested.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated: December 19, 2008

By: _____

Won Tae C. Kim, Reg. # 40,457
(858) 651 6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502